VZCZCXRO4521
PP RUEHAG RUEHROV
DE RUEHMD #2055/01 3041718
ZNY CCCCC ZZH
P 311718Z OCT 07
FM AMEMBASSY MADRID
TO RUEHC/SECSTATE WASHDC PRIORITY 3727
RUEAHLC/HOMELAND SECURITY CENTER WASHINGTON DC PRIORITY
RUEILB/NCTC WASHINGTON DC PRIORITY
INFO RUCNMEM/EU MEMBER STATES COLLECTIVE
RUEHLA/AMCONSUL BARCELONA 3153
RUEAIIA/CIA WASHDC
RUCNFB/FBI WASHDC

C O N F I D E N T I A L SECTION 01 OF 05 MADRID 002055

SIPDIS

SIPDIS

FOR S/CT (MCKUNE), NCTC AND DHS

E.O. 12958: DECL: 10/30/2017
TAGS: KVPR PTER PREL PGOV PINR CIVS ASEC KHLS SP
SUBJECT: SPAIN: RESPONSE TO S/CT REQUEST FOR INFORMATION ON HOST GOVERNMENT PRACTICES - INFORMATION COLLECTION, SCREENING, AND SHARING

REF: STATE 133921

MADRID 00002055 001.2 OF 005

Classified By: DCM Hugo Llorens for Reasons 1.4 (b) and (c)

¶1. (SBU) Embassy Madrid offers the following responses to REFTEL request for information on the government of Spain's policies toward and capabilities for collection of biographic and biometric data for terrorist screening purposes. For ease of reading, we have opted to rewrite each question set above the appropriate responses in the body of the report. The below information represents the current understanding of our Mission interagency team, both what we already knew before the S/CT request came in, and what we were able to collect and learn during the reporting period. We have noted that some gaps still remain and will make it a priority to fill in the blanks as we continue to engage with a Spanish government that has become one of the USG's key partners in the fight against terrorism.

¶2. (C) A. Watchlisting: If host government maintains a "watchlist," how many records does the watchlist contain, and how many are terrorist-related? Which ministry or office maintains the watchlist?

-- The GOS does not currently maintain a separate terrorist watchlist at the border, but Spain is part of the Schengen Information System (SIS), and has access to EU holdings. The GOS has plans to implement the SIS at ports of entry beginning in 2009. On September 17, the U.S. and Spain signed a cutting-edge bilateral information sharing agreement covering known and suspected terrorists as envisioned under HSPD-6. Under this agreement, the Spanish Ministry of Interior will be responsible for supplying Spanish data into the U.S. Terrorist Screening Center database/watchlist, and will conversely be the recipient of TSC data.

¶3. (C) B. Traveler Information Collection: What are the country's policies (legislation, mandates, etc.) on collecting information from travelers arriving in the country? Are there different policies for air, sea, and land entry and for domestic flights? Who collects traveler information? What are the policies of the collecting agency to share that information with foreign governments? Does the host government collect Passenger Name Record (PNR) data on incoming commercial flights or vessels? Is this data used for intelligence or law enforcement purposes to screen travelers? Does host government have any existing treaties

to share PNR data? If applicable, have advance passenger information systems (APIS), interactive advanced passenger information systems (IAPIS), or electronic travel authority systems been effective at detecting other national security threats, such as wanted criminals?

-- Currently, Spain only collects the limited information requested on arrival cards, but this information is not entered into a computer database. What information is gathered and kept is shared within the EU and the SIS. Passports are scanned upon arrival (this is still a test project) to verify if there has been any alteration or forgery. As Spain is a part of the Schengen agreement, it does not maintain any type of passport controls upon entry or exit for all domestic travel to EU member countries (except the United Kingdom). Spain does not maintain any type of passport controls upon entry and exit, and does not maintain any type of travel records. Persons traveling to and from the UK are required to be screened at passport control in Spain, but Spain does not maintain these travel records. In regards to international travel, persons departing and entering Spain are required to be screened at passport control. It is our experience that Spain has not readily automated this type of information, thus making any retrieval of international travel data almost impossible. Spain on occasion maintains data if the border official encountering the traveler physically loads the traveler's information, but this is rare. Spain does not collect traveler data for persons entering Spain on land via France or Portugal, and there are no longer checks at border crossings between the countries. Persons entering Spain via Gibraltar are required to be screened at passport control, but Spain does not maintain this data. The collection of traveler information is the responsibility of the Spanish National Police, and the SNP is very willing to share this type of information. However, for the reasons enumerated above, the SNP has very

limited data available, and what exists is usually of little value. Spain does not have an Advanced Passenger Information System (APIS). On November 6, the EU Commission plans to approve a project whereby data relative to passengers arriving by air will be stored and reviewed by each member state. The proposed system will use the same fields as that used by the U.S. system. The objective of this program is to use it for both intelligence and law enforcement purposes. Spanish law enforcement implements a mechanism by which they are able to effectively detect the travel of passengers with warrants for arrest. In relation to terrorists, the mechanism is not yet in place, but is forthcoming.

¶4. (C) C. Border Control and Screening: Does the host government employ software to screen travelers of security interest? Are all travelers tracked electronically, or only non-host-country nationals? What is the frequency of travelers being "waived through" because they hold up what appears to be an appropriate document, but whose information is not actually recorded electronically? What is the estimated percentage of non-recorded crossings, entries and exits? Do host government border control officials have the authority to use other criminal data when making decisions on who can enter the country? If so, please describe this authority (legislation, mandates, etc. What are the host government's policies on questioning, detaining and denying entry to individuals presenting themselves at a point of entry into the country? Which agency would question, detain, or deny entry? How well does information sharing function within the host government, e.g., if there is a determination that someone with a valid host-government visa is later identified with terrorism, how is this communicated and resolved internally?

-- Spanish authorities use what they call a "Verifier." The SNP officer at the POE decides who will be "verified" to see whether they are under an arrest warrant of a "No-entry" into the Schengen area. This database is shared with the Civil

Guard. Spanish border control systems are being developed further under Schengen and are scheduled for implementation in 2009. Spain does not currently possess border control software. Very few travelers are tracked electronically as they enter Spain. Documents are visually checked, with more intense screening possible and done randomly and on certain flights. We estimate that fewer than 10 percent of entries and exits into Spain are recorded. Spanish border control are sworn officers of the Spanish National Police, and they are not restricted in using criminal data when making decisions on who can enter the country. However, it has been the experience of our Legatt that the principal decisonmaking factor for allowing or disallowing entry into Spain is whether or not the traveler possesses proper travel documentation. Spanish immigration, however, can and does deny entry into the country. The sharing of information between the Spanish National Police and the Spanish Civil Guard, Spain's two national law enforcement services, is problematic. The two services have strong CT missions, but generally work independent of each other and rarely share information. When the two services do share information, it is normally conducted via informal channels. Spain created the National Center for Counterterrorism Coordination in 2005, a CT collection, analysis, and dissemination hub, which serves as a terrorism coordination center for Spanish law enforcement and intelligence agencies. However, the center is still in its infancy, and the sharing of information through the center continues to be a work in progress.

¶5. (C) D. Biometric Collection: Are biometric systems integrated for all active POEs? What are the systems and models used? Are all passengers screened for the biometric or does the host government target a specific population for collection (i.e. host country nationals)? Do the biometric collection systems look for a one to one comparison (ensure the biometric presented matches the one stored on the e-Passport) or one to many comparison (checking the biometric presented against a database of known biometrics)? If biometric systems are in place, does the host government know of any countermeasures that have been used or attempted to defeat biometric checkpoints? What are the host government's policies on collecting the fingerprints of travelers coming into the country? Which agency is responsible for the host government's fingerprint system? Are the fingerprint programs in place NIST, INT-I, EFTS, UK1 or RTID compliant?

Are the fingerprints collected as flats or rolled? Which agency collects the fingerprints?

-- Biometric systems are not yet integrated into the Ports of Entry (POEs), although "Poto" biometric is used. Spain maintains biometrics (photo/fingerprint) for all Spanish nationals and holders of Spanish identity documents. The GOS plans to take fingerprints with the implementation of the SIS border controls in 2009. The Spanish National Police is responsible for managing Spain's national fingerprint system. This system is known as "SAID," and "SAID II" will soon be implemented. SAID II is meant to be more compatible with other international law enforcement partners and should greatly increase Spain's power to process raw fingerprint data. According to Legatt records, the SAID is currently NIST and INT-I compliant. The SAID II is supposed to be EFTS and, more importantly, ANSI/NIST-ITL-1-2007 compliant. Fingerprints collected are always rolled, but Spain will soon be collecting digital flats. Print data is collected by all of the various law enforcement agencies within Spain, but the SNP is responsible for serving as the central repository for fingerprint data.

¶6. (C) E. Passports: If the host government issues a machine-readable passport containing biometric information, does the host government share the public key required to read the biometric information with any other governments? If so, which governments? Does the host government issue replacement passports for full or limited validity (e.g. the

time remaining on the original passports, fixed validity for a replacement, etc.)? Does the host government have special regulations/procedures for dealing with "habitual" losers of passports or bearers who have reported their passports stolen multiple times? Are replacement passports of the same or different appearance and page length as regular passports (do they have something along the lines of our emergency partial duration passports)? Do emergency replacement passports contain the same or fewer biometric fields as regular-issue passports? Where applicable, has Post noticed any increase in the number of replacement or "clean" (i.e. no evidence of prior travel) passports used to apply for U.S. visas? Are replacement passports assigned a characteristic number series or otherwise identified?

-- Spain's public key system is shared within the SIS and with others. All full-validity passports are issued in Spain under a system very similar to ours, and Spanish Embassies and Consulates can issue a limited-validity emergency passport which, like ours, is not an e-passport. Replacement passports are recognizable because they are not issued for the full 10-year validity; they are issued for a limited validity that coincides with the validity of the passports being replaced. Spain does have procedures for dealing with habitual losers of passports, and can include significant fines. Emergency and replacement passports contain the same information as regular passports.

¶7. (C) F. Fraud Detection: How robust is fraud detection and how actively are instances of fraud involving documents followed up? How are potentially fraudulently issued documents taken out of circulation, or made harder to use?

-- Spain has robust fraud detection and follows up expeditiously on all known or suspected cases. Spain has a system very similar to ours to deal with fraudulently issued documents and to get them out of circulation. Spanish national identity documents contain fingerprints and are thus hard to illegally manufacture.

¶8. (C) G. Privacy and Data Security: What are the country's policies on records related to the questioning, detention or removal of individuals encountered at points of entry into the country? How are those records stored, and for how long? What are the country's restrictions on the collection or use of sensitive data? What are the requirements to provide notice to the public on the implementation of new databases of records? Are there any laws relating to security features for government computer systems that hold personally identifying information? What are the rules on an individual's ability to access data that homeland security agencies hold about them? Are there different rules for raw data (name, date of birth, etc.) versus case files (for example, records about enforcement

actions)? Does a non-citizen/resident have the right to sue the government to obtain these types of data?

-- Spain's privacy rules track with those of the EU. Removal and deportation records are maintained in the SIS for periods of 3 to 10 years or longer. Spain has rules in place for the collection and use of sensitive data that closely mirror our own. Generally, all of this data can be collected with or without a court order. Embassy Legatt is unaware of any type of data that is completely off-limits to the government. As in the U.S., data that is obtained via the legal process (i.e. subscriber data from Internet service providers or telecommunications companies, data intercepts, telephone intercepts, etc. is "owned" by the investigative magistrate that issued the order to obtain the data, not the law enforcement agency that is conducting the investigation. This investigative magistrate decides how the data can be used as well as who it can be shared with. Data that is collected exclusively by law enforcement can be released by that service at their own discretion. However, when an

investigative magistrate directs Spanish law enforcement to collect this type of data (i.e. voluntary interviews of persons, etc.), this information is once again "owned" by the investigative magistrate. The magistrate decides how the data can be used and with whom it can be shared. We are aware of one restriction pertaining to the use of sensitive data, specifically as it relates to national identity cards. Persons who obtain Spanish national ID cards, or what are commonly referred to as "DNI" or "NIE" cards, are required to provide personal identifying information, a photograph, and one fingerprint (right index finger). This print is supposed to be completely off-limits for general law enforcement use, and its use is supposed to be only for elimination purposes to ensure persons do not have more than one national ID card issued to them. The SNP is responsible for issuing DNI/NIE cards. In Spain, individuals can ask for police records, and non Spanish citizens have the right to sue for police records.

¶9. (C) H. Immigration Data Bases: What computerized immigration databases are used to track entries and exits? Is the immigration database available at all ports of entry (POEs)? If immigration databases are available at some POEs, but not all, how does the host government decide which POEs will receive the tool? What problems, if any, limit the effectiveness of the systems? For example, limited training, power brownouts, budgetary restraints, corruption, etc.? How often are national immigration databases updated?

-- Spain currently lacks immigration databases that track entry and exit records, but entry forms are collected at all POEs. Such systems are envisioned for implementation in 2009 as part of the SIS. SNP officers at the POEs do not know if a person has been into Spain previously unless there are entry stamps in the passport presented. If the passport is new, this information would not be known.

¶10. (C) I. Watchlist and Information Sharing: Is there a name-based watchlist system used to screen travelers at POEs? What domestic sources of information populate the name-based watchlist, i.e. names of deported persons, terrorist lookouts, criminal wants/warrants? What international watchlists do the host government use for screening individuals, e.g. Interpol or TSA No Fly lists, UN, etc.? What bilateral/multilateral watchlist agreements exist between host government and its neighbors?

-- Although Spain does not currently utilize any type of watchlist, name-based information is available at its POEs. However, this information is not readily-available to inspectors at primary entry points. Spain has access to SIS and Interpol information. As part of HSPD-6, the U.S. and Spain signed a bilateral agreement in Madrid on September 17 to share screening data on known or suspected terrorists. The U.S. Terrorist Screening Center and Spain's NCTC equivalent are working through a 90-day implementation period.

¶11. (C) J. Biometrics: Are biometric systems in place at ports of entry (air, land, sea)? If no, does host government have plans to install such a system? If biometric systems are available at some POEs, but not all, how does the host government decide which POEs will receive the tool? What biometric technologies, if any, does the host government use, i.e. fingerprint identification, facial recognition, iris

recognition, hand geometry, retinal identification, DNA-based identification, keystroke dynamics, gait analysis? Are the systems ICAO compliant? Does the host government issue a machine-readable passport containing biometric information? If e-Passports are issued, what biometric information is included on the document, i.e. fingerprint, iris, facial recognition, etc. If not, does host government plan to issue a biometric document in the future? When?

-- Biometrics are not yet in place at Spain's POEs, but are slated to be implemented in 2009. Spanish law enforcement

regularly utilizes fingerprint identification and DNA-based identification to conduct its mission. The Spanish e-passport contains computer chip technology with a digital photo and plans are to add fingerprints in 2009.

¶12. (C) K. Identifying Appropriate Partners:

-- Spain has been, is, and will continue to be a committed ally in the fight against terrorism and we have established relatively good channels of information sharing. Any watchlists that Spain currently has or may maintain in the future would not include political dissidents. Spain understands our rules on information sharing and would not share or use U.S. watchlist data inappropriately. As mentioned previously, we have already entered into a data-sharing agreement as envisioned under HSPD-6 and we will look to strengthen our bilateral cooperation through other appropriate agreements. Spain has a modern, competent, and independent judiciary system that is developed to adequately provide safeguards for the protection and nondisclosure of U.S. information. Spain's internal services do have a problem with sharing among themselves, but they are aware of their problems with stovepiping and are taking steps to streamline the flow of information across national services. Spain has numerous legal statutes that define terrorism much as we do, and even have laws on the books that are more relaxed than ours in terms of charging individuals with membership in a terrorist organization, support for a terrorist organization, and even positive comments made about a terrorist organization. The GOS has dealt with the Basque terrorist group ETA for more than 40 years and in recent years has focused on the threat from Islamic extremist terrorism in the wake of the March 11, 2004 Madrid train bombings. The fight against terrorism is the number one priority of this Mission and we will continue to engage with the GOS to improve on already excellent cooperation.
AGUIRRE